

NIH Wireless Network Policy

A. PURPOSE

This document establishes the policy for the deployment and use of wireless network technology at the NIH. It is intended to provide procedures to protect NIH resources and data from security threats, improve incident response for wireless issues, and mitigate interference among wireless technologies.

This document establishes policies for wireless network access services implemented within the NIH. It applies to all NIH personnel, contractors and visitors that have access to NIH facilities or NIH information. It applies to all wireless network access devices and technologies that provide a bridge between wireless and wired networks (hereafter “access points”), or any device that is designed to communicate with such a device via the wireless network (hereafter “access clients”).

B. BACKGROUND

Wireless network devices offer a simple, convenient, and inexpensive solution to extend network accessibility by reducing the requirements of physical infrastructure. Wireless networking removes the encumbrance of wire connections on portable devices, and can also enable laptop and handheld users the ability to travel beyond traditional network boundaries (e.g. between buildings) without losing network connectivity.

In addition to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including research correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception.

Exposure of sensitive data is not the only concern for the NIH. If improperly implemented, a wireless network allows an unauthenticated user an NIH IP address with all the benefits offered to any authenticated user. Using one of these trusted IP addresses, attacks could be launched against the NIH or any outside network accessible through NIHnet. Web sites devoted to open access points throughout the country are expanding and may eventually include open access points (“hot spots”) within the NIH.

DATE: 01/24/2003

REPLACES: NONE

ISSUING OFFICE: CIT/ODCIO 402-4457

NIH Wireless Network Policy

Since wireless network devices operate using radio signals, their proliferation at the NIH can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

This policy serves as the foundation for a comprehensive risk mitigation strategy; enhanced by published security standards, best practice documents and, where applicable, more granular IC-specific policy.

C. POLICY

1. Registration of Wireless Devices

- Registration of access clients is not required unless the same device is configured as an access point.
- All wireless network access points must be registered with a Central Wireless Device Database managed by CIT at the time of deployment in the NIH environment. CIT will provide a secure web interface for the IC Information System Security Officer (ISSO) or designated IC personnel to add, change and remove wireless devices on any NIHnet-connected network (including contractor sites).
- CIT, in cooperation with the IC ISSO, will establish general risk mitigation strategies for access points, users and client devices such as virus protection, password standards, and other preventative measures.
- Prior to deployment, access points must meet the standards of current security audits established by the CIT and the IC ISSOs and published in the "NIH Wireless Network Security Standards" document (<http://irm.cit.nih.gov/policy/wirelessStand.pdf>).
- Only approved and registered access points will be deployed within the NIH. Unapproved (rogue) devices may be removed from service by CIT in coordination with the IC's ISSO.

2. Management and Security of Access Points

- Physical Security: Access points should be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- Configuration Management: All wireless access points must be secured using an administrative password per the password requirements in the NIH Password Policy (see <http://irm.cit.nih.gov/policy/passwords.html>.) Administrators must ensure all vendor default usernames and passwords are removed from the device. Administration of the device should be prohibited from the wireless network.

NIH Wireless Network Policy

3. Broadcast Security and Encryption

- CIT, in coordination with the IC ISSOs, will provide an updated standards list that will include approved wireless technologies, current minimum encryption standards, and best practices for secure installations. (See “NIH Wireless Network Security Standards” document at <http://irm.cit.nih.gov/policy/wirelessStand.pdf>.)

4. Access to NIH Facilities and Data

- Once authenticated to an access point, users must either be routed outside the NIH firewall(s), or authenticated to an NIH network. Just as with a wired network, NIH network authentication--whether NIH-wide or IC-specific-- must satisfy prescribed login/password combinations prior to using NIH or IC-specific resources that are not normally accessible by nodes outside the NIH firewall(s).
- Access control mechanisms such as firewalls should be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks should employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

5. Naming Conventions

- Final device names are assigned during the registration process to avoid conflicts and confusion, and to aid the Incident Response Team (IRT) and IC ISSOs in identifying and locating wireless devices.
- If technology allows for the broadcast of a device name, standardized names shall appear in the broadcast description, along with any unique identifiers assigned to the unit.

6. Disruption and Interference

- All newly deployed wireless technologies must satisfy all existing and future standards as required by law or established by the NIH Spectrum Management Team (see section **F. RESPONSIBILITIES** of this policy).
- The NIH CIO, in coordination with the NIH Information Technology Management Committee (ITMC), will resolve any conflicts between wireless devices. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate.

NIH Wireless Network Policy

D. REFERENCES

1. DHHS Automated Information Systems Security Handbook (AISSP) - <http://irm.cit.nih.gov/policy/aissp.html>
2. NIH Information Technology General Rules of Behavior - <http://irm.cit.nih.gov/security/nihitrob.html>
3. NIH Limited Authorized Personal Use of NIH Information Technology Resources - <http://www1.od.nih.gov/oma/manualchapters/management/2806/>
4. DHHS Policy for IT Security for Remote Access - <http://irm.cit.nih.gov/itmra/HHS-IRM-2000-0005.html>
5. NIH Remote Access to the NIH Network - <http://www1.od.nih.gov/oma/manualchapters/acquisitions/26101-26-08/>
6. Security Guidelines for NIH Remote Access Users - <http://irm.cit.nih.gov/security/SecGui.html>
7. NIH Password Policy - <http://irm.cit.nih.gov/policy/passwords.html>
8. NIH Warning Banner Policy - <http://irm.cit.nih.gov/policy/warnbanners.html>
9. CIT Guidance for Securing Data on Portable Systems - <http://irm.cit.nih.gov/security/GuixSecuData.html>
10. NIH Wireless Network Security Standards - <http://irm.cit.nih.gov/policy/wirelessStand.pdf>
11. Privacy Act - [The Privacy Act of 1974, 5 U.S.C. § 552a \(as amended\)](#)

E. DEFINITIONS

1. **NIH Firewall** – A network device used to block unauthorized network traffic from entering NIHnet.
2. **NIHnet** – The name used to designate the NIH backbone computer network and all subnetworks attached to the NIH backbone.

NIH Wireless Network Policy

3. **Service Set Identifiers (SSID)** – A unique identifier attached to the header of packets sent over a LAWN (Local Area Wireless Network). It is primarily intended to differentiate LAWNs, but also acts as a rudimentary password.
4. **Wireless** – A technology that permits the transfer of information (active or passive) between separate points using electromagnetic waves rather than a physical connection.

F. RESPONSIBILITIES

1. **NIH Chief Information Officer (CIO)**
 - a. develops and implements NIH-wide policy for wireless devices and is ultimately responsible for the safety and security of the NIH Enterprise Network.
 - b. (or designee) must approve all exceptions to this policy.
2. **NIH Information Technology Management Committee (ITMC)**
 - a. provides broad level oversight and guidance on this policy and wireless operations.
 - b. serves as the review and advisory body for the development and implementation of the actions required by this policy.
3. **NIH Senior Information Security Officer (ISSO), CIT**
 - a. ensures the technical security of the NIH Enterprise Network.
 - b. implements this policy by providing detailed monitoring of this policy, enforcement tools, and procedures.
4. **IC CIOs** are responsible for the overall control and supervision of each IC-specific wireless implementation, and for IC compliance with this policy.
5. **IC ISSOs**
 - a. serve as IC's point of contact for receiving alerts and other notifications that result from the enforcement of this policy.
 - b. enforce compliance of this policy within their respective ICs. ICs are encouraged to designate a specific e-mail address and phone number for 24 x 7 notification.
6. **Incident Response Team (IRT)**
 - a. in cooperation with the IC ISSOs, will regularly scan the RF spectrum for vulnerable and/or unregistered wireless devices.
 - b. will coordinate with IC ISSOs in the event of a possible system compromise.
7. **NIH Spectrum Management Team**
 - a. will maintain the list of acceptable RF frequencies and wireless technologies.

DATE: 01/24/2003

REPLACES: NONE

ISSUING OFFICE: CIT/ODCIO 402-4457

NIH Wireless Network Policy

- b. will conduct periodic spectrum analysis to assess the potential impact of electromagnetic interference (EMI) from transmitters and the impact of electromagnetic emissions from wireless devices.
- 8. **Technical Assistance Support Center (TASC), CIT**, will provide educational resources and instructional materials to support the deployment of wireless technology within the NIH.

G. PROCEDURES

Registration process

At the time of deployment, all wireless devices will be registered with the Central Wireless Device Database. Registration information will include, but is not limited to, the following information:

- Contact information for owner and responsible parties
- Location of devices
- Intended use and coverage area
- Type of wireless technology deployed
- Manufacturer name and model number
- Device description
- SSID/ESSID (or equivalent)
- Hopping sequence (if applicable)
- Security checklist responses

Security Auditing and Intrusion Detection

Device installers must ensure the wireless device is properly secured prior to deployment. Once deployed, the responsible ISSO shall perform a security analysis using current wireless security methods. All wireless devices must meet the minimum security requirements dictated by NIH policies.

Incident Handling Process

Coordination between the IRT, IC ISSOs, and other designated parties will follow existing and future guidelines available through the IRT Web site.

http://irm.cit.nih.gov/security/ih_guidelines.html

H. RECORDS RETENTION AND DISPOSAL: All records (e-mail and non-e-mail) pertaining to this chapter must be retained and disposed of under the authority of NIH

DATE: 01/24/2003

REPLACES: NONE

ISSUING OFFICE: CIT/ODCIO 402-4457

NIH Wireless Network Policy

Manual 1743, "Keeping and Destroying Records, Appendix 1, NIH Records Control Schedule, Section 2800 which covers all aspects of Data Processing.

NIH e-mail messages. NIH e-mail messages (messages, including attachments, that are created on NIH computer systems or transmitted over NIH networks) that are evidence of the activities of the agency or have informational value are considered Federal records. These records must be maintained in accordance with current NIH Records Management guidelines. Contact your IC Records Officer for additional information.

All e-mail messages are considered Government property, and, if requested for a legitimate Government purpose, must be provided to the requester. Employees' supervisors, NIH staff conducting official reviews or investigations, and the Office of Inspector General may request access to or copies of the e-mail messages. E-mail messages must also be provided to Congressional oversight committees if requested and are subject to Freedom of Information Act requests. Since most e-mail systems have back-up files that are retained for significant periods of time, e-mail messages and attachments are likely to be retrievable from a back-up file after they have been deleted from an individual's computer. The back-up files are subject to the same requests as the original messages.

I. MANAGEMENT CONTROLS: The purpose of this manual issuance is to establish policy for the deployment, use, and security of wireless network technology at the NIH.

1. Office Responsible for Reviewing Management Controls Relative to this Chapter (Issuing Office):

Office of the Deputy Chief Information Officer, CIT

2. Frequency of Review (in years)

A wireless management plan is in place to address wireless security at NIH.

- *Management review of controls* relevant to wireless security will be performed on an ongoing basis as new technologies emerge and new areas of concern present themselves, and the existing management plan will be updated.
- *Security controls* applied to wireless technologies at NIH will be *reviewed annually* as part of the Government Information Security Reform Act (GISRA) review of the entire NIH security program.

3. Method of Review:

DATE: 01/24/2003

REPLACES: NONE

ISSUING OFFICE: CIT/ODCIO 402-4457

NIH Wireless Network Policy

In accordance with section **G. PROCEDURES** of this policy, the following controls are implemented. Further, NIH reviews of wireless technology security will be conducted in accordance with the NIH Wireless Network Security Standards located at <http://irm.cit.nih.gov/policy/wirelessStand.pdf>

Registration process

At the time of deployment, all wireless devices will be registered with the Central Wireless Device Database. Registration information will include, but is not limited to, the following information:

- Contact information for owner and responsible parties
- Location of devices
- Intended use and coverage area
- Type of wireless technology deployed
- Manufacturer name and model number
- Device description
- SSID/ESSID (or equivalent)
- Hopping sequence (if applicable)
- Security checklist responses

Through the use of the Central Wireless Device Database, any pertinent information about the wireless device can be provided to the reviewers, or the IRT in the event of an incident, within a short period of time.

Security Auditing and Intrusion Detection

Device installers must ensure the wireless device is properly secured prior to deployment. Once deployed, the responsible ISSO shall perform a security analysis using current wireless security methods. All wireless devices must meet the minimum security requirements dictated by NIH policies at http://irm.cit.nih.gov/security/sec_policy.html#policy

4. Review Reports are sent to: NIH Chief Information Officer